**Мобильный телефон стал неотъемлемой частью нашей жизни.**

**В нем мы храним самые важные для нас сведения: фотографии, документы, учетные записи от банков и электронной почты, конфиденциальную информацию, в том числе персональные данные и т.д.**

**Мобильные мошенники пытаются войти в доверие и вынудить вас заразить свое устройство или передать им конфиденциальную информацию (в том числе персональные данные).**

## РАСПРОСТРАНЕННЫЕ ВИДЫ МОБИЛЬНОГО МОШЕННИЧЕСТВА:

**► Сообщения о заражении мобильного телефона вредоносной программой.**

На экране телефона отображается поддельное сообщение, например: «В ходе сканирования телефона было обнаружено вредоносное программное обеспечение, требуется срочно скачать/загрузить «антивирус».

**Результат:** При загрузке «антивируса» вы рискуете загрузить вредоносную или шпионскую программу.

**► Мошенничество с помощью телефонных звонков («вишинг»).**

В ходе звонка мошенник пытается убедить вас предоставить/сообщить ему свои личные персональные данные или перевести денежные средства. При этом он просит совершить какие-либо действия во время звонка, не прерывая разговор.

**Результат:** Перевод денежных средств мошенникам (включая личные накопления и кредитные средства). Утечка конфиденциальной информации, которой могут воспользоваться мошенники в преступных целях.

**► Мошенничество по SMS, включая рассылку вредоносных ссылок («SMS-фишинг», «смишинг»).**

Призыв к действию с помощью текстового сообщения, которое вынуждает перезвонить, загрузить по ссылке вредоносную или шпионскую программу, оформить подписку или выдать персональные данные.

**Результат:** При переходе по ссылке происходит загрузка вредного или шпионского ПО. Перевод денежных средств мошенникам. Утечка конфиденциальной информации, которыми могут воспользоваться в преступных целях.

**► Сбрасывающиеся звонки. Призыв перезвонить на подозрительный платный номер.**

**Результат:** Съем денежных средств.

## РЕКОМЕНДАЦИИ ПО ТЕХНИЧЕСКОЙ БЕЗОПАСНОСТИ СВОЕГО ТЕЛЕФОНА ОТ ДЕЙСТВИЙ МОШЕННИКОВ:

!!! **Уберите автоматическое подключение к Wi-Fi и старайтесь не подключатся к публичным сетям Wi-Fi.** Они плохо защищены и через них злоумышленники могут получить доступ ко всем вашим данным;

!!! **Установите сложные пароли.** Пароль должен содержать буквы, цифры и специальные символы. Используйте уникальные пароли на разные аккаунты, приложения и сайты;

!!! **Не позволяйте посторонним пользоваться вашим телефоном;**

!!! **Не делитесь своими паролями и учетными записями.** Ими могут воспользоваться без вашего ведома;

!!! **Не вводите логины и пароли на незнакомых сайтах и чужих устройствах.** Возможна утечка паролей и учетных записей;

!!! **Используйте двухфакторную проверку на телефоне.** Удобнее и надежнее пользоваться специальными приложениями;

!!! **Используйте длинный ПИН-код,** это повысит безопасность;

!!! **Храните пороли и ПИН-коды в местах, куда злоумышленники не доберутся.** Не храните пароли на бумажных носителях, которые носите с собой, не сохраняйте в браузере, при использовании облачного хранилища создавайте максимально сложный пароль;

!!! **Отключите автозаполнение паролей на телефоне и браузерах.** Так посторонние не смогут войти в приложения, которыми вы пользуетесь;

!!! **Ограничьте/запретите доступ приложений к вашим личным данным** (к аккаунтам, фотографиям, SMS, контактам и тд.). Этим смогут воспользоваться злоумышленники;